

House File 127 - Introduced

HOUSE FILE 127

BY LOFGREN and KAUFMANN

A BILL FOR

1 An Act prohibiting employers and schools from seeking access to
2 certain online personal employee and student information and
3 providing penalties.

4 BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:

1 Section 1. NEW SECTION. 735.1 Definitions.

2 As used in this chapter, unless the context otherwise
3 requires:

4 1. "Access information" means user name, password, login
5 information, or other security information that protects access
6 to a personal internet account.

7 2. "Educational institution" means a public or nonpublic
8 elementary, secondary, or postsecondary school in this state.

9 3. "Employer" means the state of Iowa or any political
10 subdivision, board, commission, department, or institution
11 thereof, and every other person employing employees within this
12 state. "Employer" includes an agent or representative of an
13 employer.

14 4. "Personal internet account" means an account created via
15 a bounded system established by an internet-based service that
16 requires a user to enter or store access information by means
17 of an electronic device to view, create, utilize, or edit the
18 user's account information, profile, display, communications,
19 or stored data.

20 Sec. 2. NEW SECTION. 735.2 Employer prohibitions.

21 An employer shall not do any of the following:

22 1. Request an employee or an applicant for employment to
23 grant access to, allow observation of, or disclose information
24 that allows access to or observation of the employee's or
25 applicant's personal internet account.

26 2. Discharge, discipline, fail to hire, or otherwise
27 penalize an employee or applicant for employment for failure to
28 grant access to, allow observation of, or disclose information
29 that allows access to or observation of the employee's or
30 applicant's personal internet account.

31 Sec. 3. NEW SECTION. 735.3 Actions not prohibited —
32 employers.

33 1. This chapter does not prohibit an employer from doing any
34 of the following:

35 a. Requesting or requiring an employee to disclose access

1 information to the employer to gain access to or operate any
2 of the following:

3 (1) An electronic communications device paid for in whole or
4 in part by the employer.

5 (2) An account or service provided by the employer, obtained
6 by virtue of the employee's employment relationship with the
7 employer, or used for the employer's business purposes.

8 *b.* Disciplining or discharging an employee for transferring
9 the employer's proprietary or confidential information or
10 financial data to an employee's personal internet account
11 without the employer's authorization.

12 *c.* Conducting an investigation or requiring an employee
13 to cooperate in an investigation in any of the following
14 circumstances:

15 (1) If there is specific information about activity on
16 the employee's personal internet account relating to, and for
17 the purpose of ensuring compliance with, applicable laws,
18 regulatory requirements, or prohibitions against work-related
19 employee misconduct.

20 (2) If the employer has specific information about
21 an unauthorized transfer of the employer's proprietary
22 information, confidential information, or financial data to an
23 employee's personal internet account.

24 *d.* Restricting or prohibiting an employee's access to
25 certain internet sites while using an electronic communications
26 device paid for in whole or in part by the employer or while
27 using an employer's network or resources, in accordance with
28 state and federal law.

29 *e.* Monitoring, reviewing, or accessing electronic data
30 stored on an electronic communications device paid for in whole
31 or in part by the employer, or traveling through or stored on
32 an employer's network, in accordance with state and federal
33 law.

34 2. This chapter does not prohibit or restrict an employer
35 from complying with a duty to screen employees or applicants

1 for employment prior to hiring or to monitor or retain employee
2 communications pursuant to state or federal law.

3 3. This chapter does not prohibit or restrict an employer
4 from viewing, accessing, or utilizing information about an
5 employee or applicant for employment that can be obtained
6 without any required access information or that is available in
7 the public domain.

8 Sec. 4. NEW SECTION. 735.4 Educational institution
9 prohibitions.

10 An educational institution shall not do any of the
11 following:

12 1. Request a student or prospective student to grant access
13 to, allow observation of, or disclose information that allows
14 access to or observation of the student's or prospective
15 student's personal internet account.

16 2. Expel, discipline, fail to admit, or otherwise penalize
17 a student or prospective student for failure to grant access
18 to, allow observation of, or disclose information that allows
19 access to or observation of the student's or prospective
20 student's personal internet account.

21 Sec. 5. NEW SECTION. 735.5 Actions not prohibited —
22 educational institutions.

23 1. This chapter does not prohibit an educational
24 institution from requesting or requiring a student to disclose
25 access information to the educational institution to gain
26 access to or operate any of the following:

27 a. An electronic communications device paid for in whole or
28 in part by the educational institution.

29 b. An account or service provided by the educational
30 institution that is either obtained by virtue of the student's
31 admission to the educational institution or used by the student
32 for educational purposes.

33 2. This chapter does not prohibit or restrict an educational
34 institution from viewing, accessing, or utilizing information
35 about a student or applicant that can be obtained without any

1 required access information or that is available in the public
2 domain.

3 Sec. 6. NEW SECTION. 735.6 Duty or liability not created.

4 1. This chapter does not create a duty on the part of an
5 employer or educational institution to search or monitor the
6 activity of a personal internet account.

7 2. An employer or educational institution is not liable
8 under this chapter for failure to request or require that an
9 employee, student, applicant for employment, or prospective
10 student grant access to, allow observation of, or disclose
11 information that allows access to or observation of the
12 employee's, student's, applicant's, or prospective student's
13 personal internet account.

14 Sec. 7. NEW SECTION. 735.7 Penalties.

15 1. A person who violates section 735.2 or 735.4 is subject
16 to a civil penalty of not more than one thousand dollars
17 for each violation. The attorney general or the attorney
18 general's designee may maintain a civil action to enforce this
19 subsection. Any civil penalty recovered shall be deposited in
20 the general fund of the state.

21 2. An aggrieved individual may bring a civil action in
22 district court to enjoin a violation of section 735.2 or 735.4
23 and may recover not more than one thousand dollars in damages
24 in addition to reasonable attorney fees and court costs.

25 No later than sixty days before filing a civil action for
26 damages or sixty days before adding a claim for damages to an
27 action seeking injunctive relief, the individual shall make a
28 written demand of the alleged violator for not more than one
29 thousand dollars. The written demand shall include reasonable
30 documentation of the violation. The written demand and
31 documentation shall either be served in accordance with state
32 law applicable to the service of process in civil actions or
33 mailed by certified mail and addressed to the alleged violator
34 at their residence, principal office, or place of business.
35 A civil action under this subsection may be brought in the

1 district court for the county where the alleged violation
2 occurred or for the county where the person against whom the
3 civil complaint is filed resides or has their principal place
4 of business.

5 3. It is an affirmative defense to a civil action under this
6 chapter that an employer or educational institution acted to
7 comply with the requirements of state or federal law.

8

EXPLANATION

9 This bill prohibits an employer from requesting an employee
10 or an applicant for employment to grant access to, allow
11 observation of, or disclose information that allows access
12 to or observation of the employee's or applicant's personal
13 internet account. The bill also prohibits an employer from
14 discharging, disciplining, failing to hire, or otherwise
15 penalizing an employee or applicant for employment for
16 failure to grant access to, allow observation of, or disclose
17 information that allows access to or observation of the
18 employee's or applicant's personal internet account.

19 The bill prohibits an educational institution from
20 requesting a student or prospective student to grant access
21 to, allow observation of, or disclose information that allows
22 access to or observation of the student's or prospective
23 student's personal internet account. The bill also prohibits
24 an educational institution from expelling, disciplining,
25 failing to admit, or otherwise penalizing a student or
26 prospective student for failure to grant access to, allow
27 observation of, or disclose information that allows access
28 to or observation of the student's or prospective student's
29 personal internet account.

30 The bill defines "employer" as the state of Iowa or
31 any political subdivision, board, commission, department,
32 or institution thereof, and every other person employing
33 employees within this state. "Employer" includes an agent or
34 representative of an employer. The bill defines "educational
35 institution" as a public or nonpublic elementary, secondary, or

1 postsecondary school in this state. The bill defines "personal
2 internet account" as an account created via a bounded system
3 established by an internet-based service that requires a user
4 to enter or store access information by means of an electronic
5 device to view, create, utilize, or edit the user's account
6 information, profile, display, communications, or stored data.
7 The bill defines "access information" as user name, password,
8 login information, or other security information that protects
9 access to a personal internet account.

10 The bill sets out various actions which are not prohibited
11 by the bill, such as actions relating to devices or accounts
12 obtained through an employer or educational institution,
13 seeking information available in the public domain, and
14 investigating improper use of an employer's proprietary or
15 confidential information or financial data or other illegal
16 activity.

17 The bill does not create a duty on the part of an employer
18 or educational institution to search or monitor the activity
19 of a personal internet account. An employer or educational
20 institution is not liable under the bill for failure to request
21 or require that an employee, student, applicant for employment,
22 or prospective student grant access to, allow observation of,
23 or disclose information that allows access to or observation of
24 their personal internet account.

25 The bill provides that a person who violates the
26 prohibitions in the bill is subject to a civil penalty of not
27 more than \$1,000 for each violation. The attorney general or
28 the attorney general's designee may maintain a civil action to
29 enforce the penalty.

30 An aggrieved individual may bring a civil action in district
31 court to enjoin a violation of the prohibitions in the bill
32 and may recover not more than \$1,000 in damages in addition to
33 reasonable attorney fees and court costs. The bill sets out a
34 process for an aggrieved individual to serve notice and bring
35 such a civil action in district court.

H.F. 127

1 The bill establishes an affirmative defense to a civil
2 action under the bill for an employer or educational
3 institution acting in compliance with state or federal law.